AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

5200 Susan Drive, Amarillo, Texas

Case No. 2:20-MJ-72

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the NORTHERN District of TEXAS, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252, ET. SEQ.	Certain Activities relating to material involving sexual exploitation of minors

The application is based on these facts:

SEE AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

J Scott Hendricks
Applicant's signature

Scott Hendricks, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/1/2020

Lee Ann Reno
Judge's signature

City and state: AMARILLO, TEXAS

LEE ANN RENO, U.S MAGISTRATE JUDGE
Printed name and title

Print | Save As... | Attach | Reset

AFFIDAVIT OF FBI SPECIAL AGENT T. SCOTT HENDRICKS
IN SUPPORT OF SEARCH WARRANT
2:20-MJ-72

I, Special Agent, T. Scott Hendricks, of the Federal Bureau of Investigation (FBI), being duly sworn under oath, do hereby depose and state:

I am a Special Agent with the FBI, and I have been so employed since 2002. I am currently assigned to the Amarillo Resident office of the FBI in Amarillo, Texas.

My duties as a Special Agent include conducting investigations into various sexual exploitation crimes committed against children, and presenting these cases for prosecution. Most of the cases are prosecuted federally. I have conducted many investigations related to the sexual and physical abuse of children, electronically facilitated exploitation of children, possession and promotion of child pornography, and online solicitation of minors, among others.

As part of my official duties I have conducted and participated in investigations relating to the sexual exploitation of children. During the course of these investigations I have observed and reviewed examples of child pornography in various forms of media, including computer media. As part of my duties and responsibilities as a Special Agent, I am authorized to investigate crimes involving the sexual exploitation of children, including alleged violations of 18 U.S.C. § 2252(a) relating to material constituting or containing child pornography.

1. This affidavit is provided in support of an application for a search warrant for the residence of Michael Dewayne Alfred, 5200 Susan Drive, Amarillo, Texas. Through investigative efforts, including physical surveillance by other law enforcement officers, the residence has been identified as a single-story residence located at 5200 Susan Drive, Amarillo, Texas. The residence is more fully described in Attachment "A" of this affidavit, which is attached hereto and fully incorporated herein by reference.

2. The statements contained in this affidavit are based on my experience, training, and background as a Peace Officer and Task Force Officer, and on information provided to me by other law enforcement officers who have assisted in the investigation.

3. As more fully described below, I have probable cause to believe that presently and/or at the time of this warrant's execution, property which is evidence relating to 18 U.S.C. § 2252(a) relating to material constituting or containing child pornography will be found inside the residence described in Attachment "A" of this affidavit. The items I have reason to believe will be found inside the residence constitute evidence of the commission of federal offenses relating to violations of the above-referenced statute. Such items are evidence, contraband, the fruits of crime and things otherwise criminally possessed, and property designed or intended for use or which is or has been used as the means of committing a criminal offense. These items are described in Attachment "B" to this affidavit, which is attached hereto and incorporated herein.

BACKGROUND

4. With regard to persons who are sexually attracted to minors, computers, including almost all cellular telephones, basically serve four functions: production, communication, distribution, and storage.

5. Persons who transport images of child pornography can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, including those incorporated in cellular telephones, the images can also be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

6. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Cellular telephones are likewise capable of the storage and transportation of child pornography, and can easily be used, through the use of various applications, to communicate with persons with some degree of anonymity, and to possess, receive, and transport images and videos of child pornography.

7. The Internet and its World Wide Web afford persons who are sexually attracted to minors, or who simply wish to transfer obscene material to

minors, almost unlimited opportunities to communicate with minors in a relatively secure and anonymous fashion. They can also request that minors transmit to them various types of material, including child pornography, using various apps that use the Internet, or through telephone texting.

8. As is the case with most digital technology, communications by way of computer or cellular telephone can be saved or stored on the computer or cellular telephone used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer (or telephone) or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains particular software or "applications," when the computer or cellular telephone was being used to communicate with other persons, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

9. For the purpose of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives)

and internal communications devices (such as internal modems capable of sending/receiving electronic mail or fax cards) along with any other hardware stored or housed internally. Thus, "computer" refers to hardware, software and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term "computer system" is used. Information refers to all the information on a computer system including both software applications and data.

10. The term "computer hardware," as used in this affidavit, refers to all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices, peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware

(such as physical keys, locks, and dongles).

11. The term "computer software," as used in this affidavit, refers to digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

12. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that the Internet is a worldwide computer network which connects computers, including cellular telephones which constitute computers, and allows communications and the transfer of data and information across state and national boundaries. Individuals who utilize the Internet can communicate by using electronic mail (hereafter referred to as "e-mail"). E-mail is an electronic form of communication that can contain letter type correspondence and graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message header which gives information about the individual who originated a particular message or graphic, and importantly, the return address to respond to them.

13. Visual depictions and graphic files referred to below are in the form of "computer graphic files". Computer graphic files are photographs or other visual depictions that have been digitized into computer binary format. Once in

this format, graphic files can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Examples of image computer file extensions, which represent different format conventions, are "jpg," "gif," "mpg," and "avi."

14. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet.

15. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, optical, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard drives, CD-ROMs, digital video or versatile disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory cards/sticks, optical disks, flash (thumb) drives, printer buffers, smart cards, memory calculators, electronic dialers, cell phones, gaming consoles, or

electronic notebooks, as well as digital data files and printouts or readouts from any electrical, electronic, optical, or magnetic storage device).

16. "URL" or "Uniform Resource Locator" refers to Internet addresses. Each website on the Internet has a unique address called a Uniform Resource Locator, more commonly known as URL.

CHARACTERISTICS OF PERSONS WHO RECEIVE, TRANSPORT, POSSESS, AND COLLECT CHILD PORNOGRAPHY

17. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt, transportation, possession, and collection of child pornography:

a. Persons who receive, transport, possess, and collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Persons who receive, transport, possess, and collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual

media. Persons who receive, transport, possess, and collect child pornography oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Persons who receive, transport, possess, and collect child pornography often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, persons who receive, transport, possess, and collect child pornography usually maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Persons who receive, transport, possess, and collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other persons who share their interest in child pornography; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of

individuals with whom they have been in contact and who share the same interests in child pornography.

f. Persons who receive, transport, possess, and collect child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. With the ease of obtaining new images of child pornography and child obscenity by using various means available on the Internet, some persons who receive, transport, possess, and collect child pornography, or who attempt to commit these crimes, sometimes delete their images and obtain new material, in a continuing cycle. Even when they engage in this pattern of conduct, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence indicating whether a computer contains software that can be used to store images and videos on "the cloud" (remote servers), and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

18. As set forth above, probable cause exists to believe that an individual utilizing the Internet at 5200 Susan Drive, Amarillo, Texas, exhibits the

common characteristics described above of someone involved in the receipt, transportation, possession, and collection of child pornography, or the attempted receipt, transportation, or possession of child pornography. Based on the facts set forth in this affidavit I believe that the individual utilizing IP address 75.3.83.42 on 04/07/2020, as referenced herein, demonstrates the characteristics of a person who receives, transports, possesses, and collects child pornography.

SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

19. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel, I am aware that searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a) Computer storage devices (like hard drives, diskettes, tapes, laser disks, CD-ROMs, DVDs, and flash drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data

stored, and it would be impractical to attempt this kind of data search on site.

b) Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes embedded in the system, such as "booby traps,") a controlled environment is essential to its complete and accurate analysis.

20. In addition, there is probable cause to believe that cellular telephones, computers and storage devices, monitors, keyboards, and modems, are all instrumentalities of the crimes relating to the possession, transportation, or receipt of child pornography, in violation of 18 U.S.C. § 2252(a).

THE INVESTIGATION- FACTUAL BACKGROUND

21. LiveMe is a mobile service that lets users create, share and participate in live stream video broadcasts through our website and mobile app (e.g., LiveMe for Android; LiveMe for iOS). Most LiveMe account information is public, so anyone can see it. A LiveMe account profile contains a profile photo, brief "bio" written by the respective user, list of fans/followers, and any previously archived live-streamed broadcasts. LiveMe keeps archives of all user posted broadcasts, direct messages, and LiveMe account profile photos as long as a user account is active (i.e. not terminated). Archived information is retained for a limited time. LiveMe retains different types of information for different time periods. Given LiveMe's real-time nature, some information (e.g., IP logs) may only be stored for a very brief period of time. All information collected by LiveMe will be deleted if a user's account is terminated or such information (i.e. broadcasts) is deleted by the user. Some information LiveMe stores is automatically collected, while other information is provided at the user's discretion. Though LiveMe does store this information, LiveMe cannot guarantee its accuracy. For example, the user may have provided fake or anonymous account information when registering his/her account. LiveMe only requires a phone number and email address, as well as the user to input their birthdate in order to register an account.

22. On 01/03/2020, Online Covert Employee - 6765 ("OCE") – an FBI Special Agent, who is a member of the FBI Child Exploitation Task Force in Salt Lake City, Utah, was connected to the Internet in an online undercover capacity in

Salt Lake City, Utah. A software program was used to record the online activity, chats, and images identified within LiveMe. OCE was logged into the application LiveMe, in an undercover capacity, to identify individuals who were involved with the sexual exploitation of children.

23. On 01/03/2020, an individual with the LiveMe profile identifier "265821181", using the screen name "Mike420811" was found to have a sexual interest in incest/children. During the course of this online undercover session it was identified that this LiveMe user was a member of a known child pornography group titled "Wonderland". Members within this group distributed hundreds of videos of child rape, described as nude prepubescent age children, including infants and toddlers, engaged in sexual acts with adults and other children. This LiveMe user posted two "links" to the group which contained numerous videos of nude prepubescent age children engaged in sexual acts with adults and other children. OCE downloaded a video from one of these links for reference. A description of a sampling of the images downloaded from this IP address are:

Vid-20140805-WA0002.mp3	Depicts a prepubescent girl lying nude on a bed. A nude adult male wearing a clown mask is anally penetrating the girl with a large dildo.

I observed this video and it meets the federal definition of child pornography.

In the "ABOUT ME" section for this LiveMe user it stated "Lookin for those fine TX girls for fun any age any race". The OCE also communicated with this LiveMe user outside of the group one on one where he discussed fantasizing about sexually

abusing children. Highlights of the conversation between FBI OCE and LiveMe user "MIKE420811" is as follows:

- OCE: Hey I'm a perv dad with a yung daughter, no limits, USA, looking for other like minded parents, hbu?
- MIKE420811: Kids already grown and gone but always been into it
- OCE: Mmm ever been active with anyone?
- MIKE420811: Not from here
- OCE: I'm in real life, I mean in person
- MIKE420811: No just fantasy
- OCE: Too bad

24. The FBI sent a subpoena to LiveMe requesting subscriber data for this account. The response from LiveMe revealed the following:

- Username: Mike420811
- SID: 265821181
- Registration Device: iPhone11
- IP Addresses: 208.180.96.248 & 50.26.101.145 (Suddenlink)

25. The FBI sent a subpoena to Suddenlink requesting subscriber information for IP addresses used to login to this LiveMe account. Suddenlink then provided subscriber information as follows:

- **Subscriber data for 208.180.96.248**
- GRN SITE ONE LANDSCAPE

- Address: 4113 Republic Ave., Amarillo, TX 79109
- Phone: 806-463-6334
- **Subscriber data for 50.26.101.145**
- Latoria Alfred
- Address: 5200 Susan Dr., Amarillo, TX 79110
- Phone: 806367-7228

26. On 04/07/2020, Online Covert Employee - 6765 ("OCE") – an FBI Special Agent, who is a member of the FBI Child Exploitation Human Trafficking Task Force in Salt Lake City, Utah, was connected to the Internet in an online undercover capacity in Salt Lake City, Utah. A software program was used to record the online activity, chats, and images identified within LiveMe. OCE was logged into the application LiveMe, in an undercover capacity, to identify individuals who were involved with the sexual exploitation of children.

27. On 04/07/2020, an individual with the LiveMe profile identifier "224399422", using the screen name "Michelle1108" was found to have a sexual interest in incest/children. During the course of this online undercover session it was identified that this LiveMe user was a member of numerous known child pornography groups titled "Gurls Share Stuff" and many others. Members within this group distributed hundreds of videos of child rape, described as nude prepubescent age children, including infants and toddlers, engaged in sexual acts with adults and other children. This LiveMe user posted a Mega "link" to the group which contained a video of a nude prepubescent age child being sexually abused by

adults. OCE downloaded the video for reference. A description of a sampling of the images downloaded from this IP address are:

IMG_2768.MP4	Depicts a prepubescent girl lying on a bed wearing panties and a shirt. An adult male is masturbating in front of the girl, pulls her panties to the side and inserts his erect penis into her vagina.

I observed this video and it meets the federal definition of child pornography.

28. The FBI sent a subpoena to LiveMe requesting subscriber data for this account. The response from LiveMe revealed the following:

- Username: Michelle1108
- SID: 224399422
- Registration Device: iPhone11
- IP Addresses: 75.3.83.42 (AT&T), 208.18.96.248 (Suddenlink)

29. The FBI sent a subpoena to Suddenlink requesting subscriber information for IP addresses used to login to this LiveMe account. Suddenlink had provided subscriber information as follows:

- Returns to GRN SITE ONE LANDSCAPE
- Address: 4113 Republic Ave, Amarillo, TX 79109
- Phone: 806-463-6334

30. The FBI sent a subpoena to AT&T requesting subscriber information for IP addresses used to login to this LiveMe account. AT&T then provided subscriber information as follows:

- Subscriber: Michael Alfred
- Address: 5200 Susan Dr. Amarillo, TX 79110
- Phone: 806-673-7675
- Email: mikefred0811@yahoo.com

31. A public data base search for people connected to the address, email, phone number. It appears the following person may be utilizing the above mentioned LiveMe accounts:

- Name: Michael DeWayne Alfred
- DOB: XX/XX/1977
- SSN: XXX-XX-6316
- Address: 5200 Susan Dr. Amarillo, TX 79110
- Email: mikefredo811@yahoo.com, alfredo811@yahoo.com, mike0811@sbcglobal.net
- Phone: 806-673-7675

32. A public records check indicate that Michael Alfred is married to Latoria Alfred.

33. A review of the Facebook page for Michael Alfred reveals a profile picture of a baby yoda similar to the LiveMe profile picture for Mike420811.

34. Physical surveillance by Potter County Attorney Investigators place Michael Alfred residing at 5200 Susan Dr. Amarillo, and working at 4113 Republic Ave, Amarillo. It appears the device being used to connect to LiveMe is a cell phone and therefore can be used at either location.

35. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that violations of Title 18, United States Code, Section 2252(a) have been committed, and that:

a. property that constitutes evidence of the commission of a criminal offense;

b. contraband, the fruits of crime, and things otherwise criminally possessed; and

c. property designed and intended for use, and which has been used as a means of committing a criminal offense,

are located at the residence of Michael Alfred, described in Attachment "A" to this affidavit. The property to be seized pursuant to this warrant is described in Attachment "B" to this affidavit.

CONCLUSION

Based upon all of the information set forth in this application, I respectfully submit that there is probable cause to believe that, Michael Alfred, or another person residing at 5200 Susan Dr., Amarillo, Texas, is a person involved in the sexual exploitation of minors through the receipt, transportation, possession, and

collection of child pornography, and as such, this individual is likely to now be in possession of evidence of said offenses and any images and communications related thereto. There is probable cause to believe that said evidence will be found at the residence described in Attachment "A" hereto.

I respectfully request that this Court issue an order authorizing the search 5200 Susan Dr., Amarillo, Texas, more fully described in Attachment "A" of this affidavit, including any external storage structures and vehicles under the control of Michael Alfred or any other individuals located on the property, and any cellular telephones, computers, and associated devices contained therein, for the items, materials, and records more specifically identified in Attachment "B".

Further affiant sayeth not.

_/s/ *Scott Hendricks*_____
Special Agent T. Scott Hendricks
Federal Bureau of Investigation

Attested to in accordance with the requirements of Fed. R. Crim. P 4.1 by telephone, this 1st day of June, 2020, and I find probable cause.

Lee Ann Reno
LEE ANN RENO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A"
DESCRIPTION OF PREMISES TO BE SEARCHED

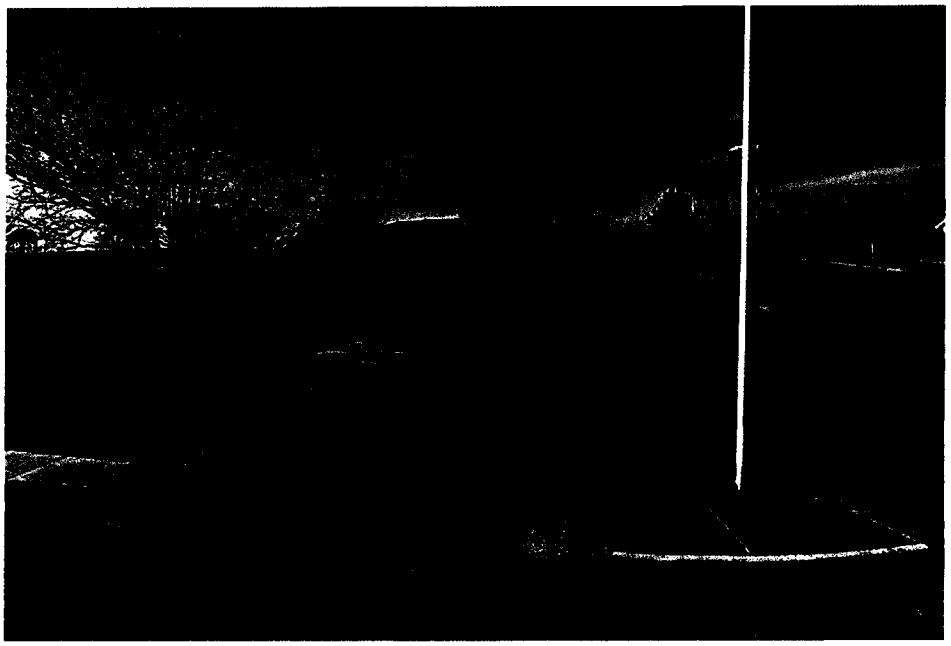
There is in Amarillo, Randall County, Texas, a residence located and described as follows:

5200 Susan Dr., Amarillo, Texas.

Further described as follows:

A brown brick single family residence with a brown shingled roof and brown painted trim. The house sits on the west side of the street and faces east. The garage door is white in color and the numeral "5200" is affixed to the house above the garage door.

Said suspected place, in addition to the foregoing description, also includes all other buildings, structures, places and vehicles on said premises and within the curtilage, that are found to be under the control of the suspected party named below and in, on, or around which said suspected party may reasonably reposit or secrete property that is the object of the search requested herein.



ATTACHMENT "B"
ITEMS TO BE SEARCHED FOR AND SEIZED

Instrumentalities of violations of 18 U.S.C. § 2252(a), located at 5200 Susan Dr., Amarillo, Texas, in any form wherever it may be stored or found, including, but not limited to:

1. Any computer, computer system and related peripherals, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to, computer hardware, software, diskettes, backup tapes, CD-ROMs, DVDs, flash memory devices, cellular telephones, gaming consoles, and other storage mediums; any input/output peripheral devices, including but not limited to, passwords, data security devices and related documentation, and any hardware/software manuals;

2. Information or correspondence pertaining to violations of Title 18, United States Code, Section 2252(a), which makes it a federal offense for Any person who—

   (1) Knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or mails, any visual depiction, if—

      (A) The producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

      (B) Such visual depiction is of such conduct;

   (2) Knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility

of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if—

(A) The producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) Such visual depiction is of such conduct.

3. Credit card information, including, but not limited to, bills and payment records, relevant to any activity in relation to any of the offenses referenced in Paragraph 2;

4. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

5. Records or other items which evidence ownership or use of computer equipment, telephones, or electronic storage media found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

6. Any communications of any person, any computer programs or applications for computers or cellular telephones which are used to communicate online with other persons, which constitutes the possession, receipt, or transportation of child pornography; and

7. All computer/digital files and records which are relevant to making a determination as to the identity of the person who used a particular computer or other device to possess, receive, or transport images and/or videos of child pornography.

When searching the Subject Premises, it is likely that Apple brand devices, such as iPad or iPhones, will be found because records from LiveMe indicate the device used was an iPhone 11. I know from my training and experience and my review of publicly available materials published by Apple that those Apple devices can enable what is referred to as "Touch ID," a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID

sensor, a round button on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numeric password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to any Apple devices found at the Subject Premises while executing the search warrant. The government may not be able to obtain the contents of the Apple devices if those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID,

and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

In consideration of the foregoing, I respectfully request that this Court issue an order authorizing the search of 5200 Susan Dr. Amarillo, Texas, more fully described in Attachment "A" of this affidavit, and any cellular telephones, computers, and associated devices contained therein, for the items, materials, and records more specifically identified in Attachment "B."